**Appln No. 09/892,240**
**Amdt date August 29, 2005**
**Reply to Office action of** June 29, 2005

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Currently Amended) A cryptography engine for performing cryptographic operations on a data block, a first portion of the data block occupying a first position and a second portion of the data block occupying a second position, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

a two-level multiplexer circuitry including a multiplexer on a first level coupled to a multiplexer on a second level, ~~wherein the two level multiplexer circuitry avoids swapping of data loaded from a previous round of cryptographic processing without incurring an extra clock cycle~~;

expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to [[a]] the first portion of the data block occupying the first position;

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the first portion of the data block, wherein the multiplexer on the first level selects initial input data responsive to a first signal, and the multiplexer on the second level receives and associates, in response to a second signal,

feedback data from a previous round of cryptographic processing, with the second position, for a next round of cryptographic processing ~~whereby altering the second bit sequence performs cryptographic operations on the data block~~.

2. (Original) The cryptography engine of claim 1, further comprising an Sbox configured to alter a third bit sequence corresponding to the portion of the data block by compacting the size of the third bit sequence and altering the third bit sequence using Sbox logic.

3. (Original) The cryptography engine of claim 1, wherein the cryptography engine is a DES engine.

4. (Original) The cryptography engine of claim 1, wherein the multiplexer circuitry comprises two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level.

5. (Original) The cryptography engine of claim 1, wherein the first bit sequence is less than 32 bits.

6. (Original) The cryptography engine of claim 1, wherein the first bit sequence is four bits.

7. (Canceled)

8. (Original) The cryptography engine of claim 1, wherein the expansion logic and the permutation logic are associated with DES operations.

9. (Original) The cryptography engine of claim 1, wherein the key scheduler performs pipelined key scheduling logic.

10. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a plurality of stages.

11. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a determination stage.

12. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a shift stage.

13. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a propagation stage.

14. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a consumption stage.

15. (Currently Amended) An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block, a first portion of the data block occupying a first position and a second portion of the data block occupying a second position, the integrated

circuit layout providing information for configuring the cryptography engine, the integrated circuit layout comprising:

a key scheduler configured to provide keys for cryptographic operations;

a two-level multiplexer circuitry including a multiplexer on a first level coupled to a multiplexer on a second level, ~~wherein the two-level multiplexer circuitry avoids swapping of data loaded from a previous round of cryptographic processing without incurring an extra clock cycle~~;

expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to [[a]] the first portion of the data block occupying the first position;

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the first portion of the data block, wherein the multiplexer on the first level selects input data responsive to a first signal, and the multiplexer on the second level receives and associates, in response to a second signal, feedback data from a previous round of cryptographic processing, with the second position, for a next round of cryptographic processing ~~whereby altering the second bit sequence performs cryptographic operations on the data block~~.

16. (Original) The integrated circuit layout of claim 15, further comprising an Sbox configured to alter a third bit sequence corresponding to the portion of the data block by

compacting the size of the third bit sequence and altering the third bit sequence using Sbox logic.

17. (Original) The integrated circuit layout of claim 15, wherein the cryptography engine is a DES engine.

18. (Original) The integrated circuit layout of claim 1, wherein the multiplexer circuitry comprises two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level.

19. (Original) The integrated circuit layout of claim 15, wherein the first bit sequence is less than 32 bits.

20. (Original) The integrate circuit layout of claim 15, wherein the first bit sequence is four bits.

21. (Canceled)

22. (Original) The integrated circuit layout of claim 15, wherein the expansion logic and the permutation logic are associated with DES operations.

23. (Original) The integrated circuit layout of claim 15, wherein the key scheduler performs pipelined key scheduling logic.

24. (Original) The integrated circuit layout of claim 15, wherein the key scheduler comprises a plurality of stages.

25. (Original) The integrated circuit layout of claim 15, wherein the key scheduler comprises a determination stage.

26. (Original) The integrated circuit layout of claim 15, wherein the key scheduler comprises a shift change.

27. (Original) The integrated circuit layout of claim 15, wherein the key scheduler comprises a propagation stage.

28. (Original) The integrated circuit layout of claim 15, wherein the key scheduler comprises a consumption stage.

29-40. (Canceled).